ELECTRONIC VOTING APPARATUS, SYSTEM AND METHOD

This Application claims the benefit ~~of U.S. Provisional Patent Application Number 60/198,704 filed April 20, 2000~~, of U.S. Provisional Patent Application Number 60/245,596 filed November 3, 2000, of U.S. Provisional Application Number 60/252,012 filed November 20, 2000, of U.S. Provisional Application Number 60/253,480 filed November 28, 2000, of U.S. Provisional Application Number 60/253,778 filed November 29, 2000, of U.S. Provisional Application Number 60/_____ filed November 30, 2000, entitled "Chad-less Electronic Election Process and Method with or without Smart Card, Rev. D, November 30, 2000," and of U.S. Provisional Application Number 60/_____ filed December 7, 2000, entitled "Chad-less Electronic Election Process and Method with or without Smart Card, Rev. E, December 7, 2000."

The present invention relates to voting apparatus, systems and methods and, in particular, to electronic voting apparatus, systems and methods having at least two independent vote recording means.

Background:

Current election processes using paper cards and/or ballots have been subject of controversy because of questions concerning their accuracy, potential for voter confusion, and potential for fraud. This is true for machine voting as well as for hand-marked ballots or punch card ("chad" or "chip" removal type) ballots, whether counted by optical scanning or mechanical scanning, which introduce the additional difficulty of determining what is and is not a voted ballot due to incomplete or partial marking of a box or spot or due to the partial or incomplete punching out of a chad or chip. The accuracy and integrity of the voting process and of the counting of ballots is of great concern in any election. As is perhaps most convincingly evidenced by the events surrounding the United States Presidential Election for the year 2000, and particularly in the State of Florida, the lack or perceived lack of accuracy and integrity can cause fear, doubt, distrust and divisiveness and can undermine

confidence in government and its institutions.

While some of the foregoing is alleviated by conventional mechanical and more recently by computer-based electronic voting machines utilizing proven and applicable means of data entry such as special keyboards or touch-screens that have been constructed for conventional electronic voting machines, these do not allow or provide any way for personal checking of votes cast to increase the voter's confidence. While the use of computers for vote tabulation and record keeping for each voting machine and/or election can be done with almost zero error, voter confidence in the process is still a subject to be considered. A particular concern relates to the nature of records stored in electronic and magnetic form which are intangible and can be changed without leaving any evidence thereof.

In addition to potential machine and human error, present election and ballot systems do not provide any traceable record for the election choices of individual voters. While the secrecy of each personal ballot is important for various reasons and must be maintained, a voting system and method that would provide confirmation of his or her voting choice(s) to each individual voter and that would further allow the individual voter to compare what has been tallied during the election as his vote to such confirmation would be extremely useful and increase confidence in the integrity and accuracy of the outcome of the voting.

The following cannot be easily addressed to eliminate potential human error and the possibilities for mischief or tampering with conventional voting systems and methods:

1. Voter registration verification when the voter shows up at the polls to vote may be very strict or may be loose, without any uniform or satisfactory standard. Conventional systems simply lack any simple means to verify registration electronically and instantly before the voter is allowed to vote. This lack of certainty is magnified in the case of "provisional" ballots, as well as in the case of "domestic absentee" and "overseas absentee" ballots, particularly when such ballots are challenged.

2. The voter does not have any record of his voting selections. There is currently no sure way to allow the voter to verify and have confidence that the

vote he/she cast has indeed been tallied properly.

3. If an electronic voting booth is used, there is no feasible way to challenge or recount the voting records since the votes are accumulated electronically in electronic memories and, if stored as individual records, are stored in a random order to preserve voter anonymity. Voting machines, and particularly electronic voting machines wherein an intangible electronic or magnetic record may be altered (either intentionally or accidentally) without any telltale evidence thereof, must be totally devoid of possible tampering or other problem in order that the confidence of the voting public and of each individual voter can be preserved.

In view of the recent problems and issues in properly and accurately counting votes in the U.S. Presidential election, voters are likely asking questions such as:

How do you know that your paper, electronic, or mechanical ballot or vote was actually counted? And that it was counted correctly?

Are you comfortable that multiple voting (i.e. the old saying, "Vote early! Vote often!") has really been eliminated?

Are you sure that your absentee ballot or overseas absentee ballot was counted? And that it was counted correctly?

Are you sure that provisional ballots are properly verified and qualified, and then are counted correctly?

Can you be sure that the vote count in extremely close election, e.g., an election where the difference is a mere hundreds of votes out of many millions of votes cast or one or two votes out of several thousands of votes cast, is really correct and legitimate?

It would be desirable to have a voting apparatus, system and method that could substantially eliminate doubts and fears, whether real or imagined, concerning the accuracy and integrity of the voting apparatus, system and method. People who are among those that do not or cannot trust a voting machine or system completely, whether it utilize an electronic or mechanical voting machine, or marked or punched paper ballots, would be more likely to trust the voting system if it was "transparent," i.e. if the voting system provided a way for each individual vote to be independently

verified. Of course, transparency should be provided without compromising the secrecy of any individual vote or the confidentiality of the voting booth.

Accordingly, there is a need for a voting apparatus, system and method that provides at least two independent means for recording and counting votes.

To this end, the voting apparatus of the present invention comprises a processor for processing voting information and providing a voting session identifier, a display coupled for receiving voting information from the processor, a voter interface for receiving voting selections made by a voter and coupling same to the processor. The processor provides a voting record including the voting selections. A memory is coupled to the processor for storing the voting record and the voting session identifier; and a means is coupled to the processor for storing the voting record and the voting session identifier in a tangible medium separate from the memory.

According to another aspect of the invention, a voting system comprises a computer for tabulating voting records, at least one voting machine, and means for communicating a voting record from the at least one voting machine to the computer for tabulating the voting record. The voting machine comprises a processor for processing voting information and providing a voting session identifier, a display coupled for receiving voting information from the processor, a voter interface for receiving voting selections made by a voter and coupling same to the processor which provides the voting selections in the voting record, a memory coupled to the processor for storing the voting record and the voting session identifier and means coupled to the processor for storing the voting record and the voting session identifier in a tangible medium separate from the memory.

According to another aspect of the invention, a method for voting comprises:

initiating a voting session;

providing an identifier for the voting session;

creating a voting record including the voting session identifier and voting selections made by the voter during the voting session;

storing the voting record including the voting session identifier and the voting selections in a memory; and

storing the voting record including the voting session identifier and the voting selections in a tangible medium separate from the memory.

BRIEF DESCRIPTION OF THE DRAWING

The detailed description of the preferred embodiments of the present invention will be more easily and better understood when read in conjunction with the FIGURES of the Drawing which include:

FIGURE 1A is a schematic block diagram of an exemplary embodiment of a voting apparatus and system according to the invention and utilizing the method of the invention;

FIGURE 1B is a schematic block diagram of an alternative exemplary embodiment of a voting apparatus and system according to the invention and utilizing the method of the invention;

FIGURE 2 is a schematic block diagram of voting apparatus according to the invention and utilizing the method of the invention, and FIGURE 2A illustrates exemplary tangible receipts therefrom;

FIGURE 3 is a schematic flow diagram illustrating the voting method according to the invention;

FIGURE 4 is a schematic flow diagram illustrating the voting method according to the invention in greater detail;

FIGURES 4A-4D are schematic flow diagrams illustrating further details and alternatives for the voting method of FIGURES 3 and 4; and

FIGURE 5 is a schematic diagram illustrating a redundancy feature of the invention.

In the Drawing, where an element or feature is shown in more than one drawing figure, the same alphanumeric designation may be used to designate such element or feature in each figure, and where a closely related or modified element is shown in a figure, the same alphanumerical designation primed may be used to designate the modified element or feature. It is noted that, according to common practice, the various features of the drawing are not to scale, and the dimensions of the various features are arbitrarily expanded or reduced for clarity.

DESCRIPTION OF THE PREFERRED EMBODIMENT

FIGURE 1A is a schematic block diagram of an exemplary embodiment of a voting apparatus and system 10 according to the invention and utilizing the method of the invention. The present invention addresses the problems and challenges set forth above with a voting machine VM that includes a logical use of a computer or processor in conjunction with firmware and/or other hardware. In particular, the processor provides a unique identifier for each voting session that is associated with the voting record of that voting session. A printer LP provides a tangible record or receipt of each voter's voting session and the voting session identifier. An optional smart card or secured memory card SC or other card or device with an embedded electronic chip provides a suitable amount of memory for storing voting information including but not limited to a record of the voter's voting session and the voting session identifier. The foregoing facilitates the accomplishing of the goals of a fast, low cost, and secure transparent voting system.

As used herein, "smart card" refers to an article having at least a memory capable of storing information. Typically, a smart card includes an electronic memory device, such as a semiconductor die or chip including an electronic memory circuit, attached to or embedded in a substrate of convenient size for handling and for printing desired indicia or other information on the surfaces thereof. Smart cards may also include other electronic devices such as processors, transmitters and receivers, as is conventional for providing a desired degree of security, for communicating information to and from the memory of the smart card, and for processing the information such information. Also typically, the card is about the size of a conventional credit card or the like, but may be larger or smaller. Smart cards are sometimes referred to by other names, such as chip cards and access cards.

As used herein, "transparent" and "transparency" refer to a voting apparatus, system or method that provides a way for each individual vote to be verified independently of the accumulated voting result(s). Preferably, transparency should be provided without compromising the secrecy of any individual vote or the privacy and confidentiality of the voting booth. More preferably, transparency can be provided

that does not rely upon the security of official voting records or the actions of any individual, even an election official.

One or more voting machines VM-1, VM-2, ... VM-n are provided for voters to enter and to cast their votes, such as for candidates for office, or for or against public questions, referenda, constitutional amendments and the like, in accordance with governing law. Voting machines VM-1, VM-2, ... VM-n may be together at a common location, e.g., a polling place, or may be dispersed in any convenient number of places. Operatively associated with each of voting machines VM-1, VM-2, ... VM-n is a decoder reader/writer RW-1, RW-2, ... RW-n, respectively, into which is inserted an optional smart card SC-1. SC-2, ... SC-n each containing at least an electronic chip providing a memory of suitable capacity.

In order to vote, each voter must insert an optional smart card SC into reader/writer RW or otherwise enter a voter identification number into voting machine VM to activate voting machine VM to allow voting. The card or tag or device SC with embedded electronic memory chip preferably has security features so that the memory chip cannot be tampered with. Typically, information stored in smart cards SC may include a voter identification or serial number, e.g., relating to the rolls of registered voters, and/or voter name and address or other identifying information, identification of the voting district and/or polling place for which the smart card is valid, and/or the date of the election for which the smart card is valid, and/or a security code representative of any one or more of the foregoing by which validity and authenticity of the smart card may be validated.

It is noted that while the voter identifier and voting session identifier may be referred to as "numbers," it is not intended that such be limited to numerical characters, but any alphanumeric, numeric or symbols may be utilized in such identifier(s). Further, while such identifiers may also be referred to as "serial numbers," they may not be numbers or true serial numbers in a numerical or other sequence, but may be in any order or in no identifiable order. Unlike a conventional bar-code or magnetic stripe card, which is easily tampered with, the secure memory or smart card SC cannot be readily tampered with or copied. This is an important difference provided by utilizing a smart card SC as a medium for both verification of

voter identification as well as record keeping of the votes cast. Either a contact type smart card SC or a contact-less (wireless) type smart card may be utilized. Typical contact type and wireless (contact-less) type cards suitable for smart card SC are available from many sources. For example, cards employing electronic chips such as types SLE4442 and SLE4428 are available from Siemens located in Germany. Microprocessor chip cards available from Atmel Corporation located in Colorado and "Mifare" wireless/contact-less cards contain an electronic chip from Philips located in the Netherlands or from Siemens.

Smart card decoding reader/writer devices RW available with suitable firmware utilizing standard smart card reading and/or coding protocols can be utilized or may be modified to provide additional security. A typical decoder reader/writer unit RW is, for example, similar to those made for access control applications by Avante International Technology, Inc. located in Princeton, New Jersey, Fargo Electronics, Inc., of Eden Prairie, Minnesota, and others, is suitable for this type of secure voting system application. Devices RW need only write a record of voting information to the memory of smart card SC, which may be a blank card issued to each voter at the polling place or otherwise, or have information as described above stored therein, in accordance with the invention. Device RW need not be able to read information stored in the memory of smart card SC unless it is desired to have information stored therein that is to be utilized by voting machine VM in connection with the process of allowing a particular person to vote, e.g., such as a name, password or other personal identifier, or other information as described above.

A processor within voting machine VM employs application specific computer software or an applications shell in conjunction with a standard relational data base computer program to operatively function with decoder reader writers RW-1, RW-2, ... RW-n for reading data stored in the memory thereof and for writing data to be stored in the memory thereof. In addition, the processor also includes or has associated with it a random number generator or pseudo-random number generator or a list or sequence of unique numbers that are utilized to provide a unique voting session identifier to the voting session of each voter. Processor P may associate such voting session identifier with the voting session either at the

commencement thereof or at the conclusion thereof or at any other convenient time substantially contemporaneous therewith. The computer software for processor P is typically similar to that employed in access control systems such as the trade-show retrieval systems and access control systems available from Avante International Technology, Inc. located in Princeton, New Jersey. and from others. Typically, such software utilizes the "Visual Basic" programming language and a relational data base such as the "Access" data base, both of which are available from Microsoft Corporation located in Redmond, Washington, and may be stored on any convenient medium, such as software stored on a floppy disk or a hard drive or as firmware stored in an electronic memory or the like. The flow chart of an exemplary embodiment of such voting system and computer program is described, for example, in relation to FIGURES 3-5 below.

Also operatively associated with each of voting machines VM-1, VM-2, ... VM-n is a respective printer LP-1, LP-2, ... LP-n, respectively, for providing a respective tangible voting record PR-1, PR-2, ... PR-n, such as a printed receipt, for each voter at the conclusion of his voting. Each voting record PR-1, PR-2, ... PR-n includes the randomly assigned identifying or serial number unique to the particular voting session and a listing of the votes that the voter has cast (the voting record) that is identical to the voting record and identifying number stored in voting machine VM. The information (voting record and voting session identifier) that is printed on the printed voting receipt PR is identical to the information written into the memory of smart card SC. As a result, there are three separate and independent identical records of the voter's votes and voting session identifier, i.e., one stored in the memory (memories) of voting machine VM, one stored in the memory of smart card SC, and one printed of the voting receipt PR.

Voting machines VM may store an individual voting record for each voter or may simply accumulate the cumulative voting results as each voter casts his ballot, thereby having no record of individual voting, or may store both. Preferably, such voting record and voting session identifier are stored in the at least two independent non-volatile memory devices of voting machine VM, only one of which is typically coupled to the central computer 12 at the time for transferring voting records thereto.

Preferably, the voting information stored in the smart card SC is written over any identifying information relating to the particular voter or such information is erased by voting machine VM, thereby assuring that identity of the voter cannot be ascertained from the information stored in voting machine VM, in smart card SC and on printed receipt PR

Each voter deposits his smart card SC into a secure collection box CB before leaving the polling place (if voting machine VM and/or smart card encoder RW do not automatically collect smart card SC, which is preferable) and the voter retains the printed voting receipt. The smart cards SC in the secure collection box CB are an independent and separate re-countable electronic record of the voting, i.e. of each vote cast. Preferably, all three independent records, voting machine VM, smart card SC and printed receipt identify the voting record of the particular voter by the same unique voting session identifier which, because it is randomly assigned, is not and cannot be associated with the personal identity of the voter. Two independent identical records of the voting are held securely by the voting authorities, i.e. those in the voting machine VM and those in smart cards SC, while the third is held by the individual voters.

FIGURE 1B is a schematic block diagram of an alternative exemplary embodiment of a voting apparatus and system 10' according to the invention and utilizing the method of the invention. Voting system 10' is in all respects like voting system 10 of FIGURE 1A described above, except that smart card encoder RW and smart cards SC are not utilized. To the extent that smart cards SC may have been utilized to verify voter information and/or initiate a voting session on voting machine VM, such is accomplished in the system 10' of FIGURE 1B by an election official, as is conventional, or by the voter entering a number or other identifier or identifying information into voting machine VM, or by any other suitable arrangement.

At the conclusion of a voter's voting session, voting machine VM stores the voting record of a voting session and the voting session identifier associated therewith by its processor in its internal memory or memories and provides same to local printer LP which provides a tangible record PR, e.g., in the form of a printer\d receipt PR, to the voter. Note that system 10' still provides at least two independent and separate

identical voting records for each voting session and that these are associated with a voting session identifier by which vote tabulation may be verified independently and on a vote-by-vote basis. In particular, any voter may utilize the voting session identifier on his printed receipt PR to check the published vote results 16 to verify that his vote has been correctly recorded, thereby providing transparency of voting results 16.

With respect to both FIGURES 1A and 1B, at the end of the prescribed period for voting, e.g., when the polls close, voting machines VM are coupled to a central computer 12 and communicate either the accumulated voting result or individual voting records, or both, to central computer 12 which then combines the voting data from all of voting machines VM to tabulate and produce vote results 16. Typically, central computer 12 would be located in a secure area or facility, such as a county or state election office, or both. Where plural voting machines VM are located in close proximity, such as at one polling place or in a central facility to which they are brought at the conclusion of voting, communication by such machines with computer 12 may be through a hub 14, such as a local communication hub, a local area network, a server, the public telephone network, an electrical cable, or the like, or the memory or memories M may be removed from the voting machine VM and inserted into a reader associated with computer 12 for reading the voting results stored in such memory or memories M.

It is noted that the present invention provides complete freedom to the voting (election) authorities as to how and when the voting data is communicated to the central computer 12. It may be communicated essentially in real time as each vote is cast, or at the end of each voting session, i.e. immediately and sequentially, or may be communicated periodically either through out the appointed period for voting or at the conclusion of voting, either from the voting machines while still at the polling places or from a central or other facility to which the voting machines VM are transported. Vote results 16 may be announced or may be posted on the Internet 20 or otherwise communicated as is desirable and convenient, either as cumulative results and/or as a collection of individual voting records. Note that where the results are published as individual voting records with the voting session identifier associated

therewith, the results are 100% transparent because each individual voter may use the voting session identifier printed on his tangible receipt to check the voting record posted against that on the printed receipt.

For security and confidentiality, voting information communicated from one apparatus to another, whether such is in a common location or in separate or distant locations, is preferably encoded or encrypted, such as by public key and/or private key encryption or other encryption, as is conventional. Even where the voting information is communicated over communication links to which an unauthorized person may gain access, such as public telephone lines, radio communication or the Internet, the apparatus according to the present invention provides additional security because there is always at least one separate set of records stored in the memories of smart cards SC against which the otherwise communicated voting information can be compared and verified. Thus, whether the election is local, regional, statewide or nationwide, the arrangement of the apparatus of the invention is arranged for avoiding and circumventing any possible tampering and/or hacker attack. Of course, transporting the voting machines to a central facility with appropriate security avoids the possibility of tampering or hacking.

In the event any question arises as to the outcome of the voting, such as where the result is a very close or where the integrity of the primary vote results 16 are challenged or questioned, a parallel and independent counting of the vote may be made utilizing the collected smart cards SC collected in secure collection box CB. All the collected cards CB are processed through and are read by a smart card reader 20 and the voting results, either as a cumulative vote result or as a collection of individual voting records, or both, are produced as vote result 22 which is available for comparison to the primary vote result 16.

In accordance with the invention, the collected set of individual voting records from the primary vote result 16 and/or the backup vote result 22, may be made available, such as via the Internet 20, so that an individual voter V can log on to an election web site and, using the unique voting session identifying number recorded on his printed receipt PR, verify that his vote as printed on his confirmatory receipt PR has in fact been accurately recorded and tallied in the vote results 16 and/or 22.

The present invention provides complete transparency to the voting process because every voter receives positive confirmation that his vote has been properly recognized and recorded before he leaves the polling place, and because any voter V can verify that his vote was tallied in the vote results 16, 22. Moreover, voting confidentiality is maintained because the only information that can associate any voter and his vote is the randomly assigned unique voting session identifier that is unrelated to his personal identity. Further, voting integrity is improved because at least two separate and independent, but identical, records of the voting are provided and can be independently tallied and compared in case of challenge or question. Should vote tampering or other illegal practice be suspected or alleged, any voter can confirm whether such is the case by comparing the posted record of his voting record posted on the Internet election web site with his individual printed receipt PR.

Where voting machines VM maintain records of each individual vote, authorities can cross compare vote-by-vote using the unique voting session identifier assigned to each voter's voting session and voting record without knowing or being able to ascertain the identity of the individual voter. Such comparison can be to the voting records stored in one of the preferably two independent memories of voting machine VM or to the printed voting record receipt PR of an individual voter, or both, or to the voting records stored on the collected smart cards SC, if utilized. Moreover, such checking and comparison is private, e.g., whether by voting officials, or the public, e.g., via the Internet, because the voting session identifiers are preferably not related to voter identity.

FIGURE 2 is a schematic block diagram of voting apparatus VM according to the invention and utilizing the method of the invention. Voting machine VM includes a processor P for processing information relative to a voter and/or voting and for providing a voting session identifier, a non-volatile memory M for storing and providing such information, a display unit DU for displaying information to the voter, and a voter interface VI whereby the voter can enter information into voting machine VM for processor P and/or memory M. It is noted that the components of voting machine VM are similar to the components of a personal computer and so a conventional personal computer, with or without modification, may be utilized in

voting machine VM, although it is likely that conventional computer components, particularly processor P and memory M, may be utilized in conjunction with displays DU and input devices VI adapted to or customized for the voting machine application, for example, for ruggedness, resistance to tampering and/or abuse. In addition, processor P includes a function for providing unique voting session identifiers for each voting session, for example, a random-number or random-character generator RNG or a look-up table or other suitable generator.

Memory M may also be of any suitable non-volatile memory type. Suitable memory devices include floppy disks, computer hard disk drives, writeable optical disks, memory cards, memory modules and flash memory modules (such as those utilized in electronic cameras), magnetic and optical tapes and disks, as well as semiconductor memories such as non-volatile random-access memory (RAM), programmable read-only memory (PROM), electronically erasable programmable read-only memory (EEPROM) and the like. Memory M or a separate memory contains the operating system, data base and application software that operates processor P as voting machine VM.

Alternatively, various programming information, a voting session identifier generator or list, voting information, candidate and office information and the like may be provided in firmware, such as in an EPROM, which provides additional resistance to tampering and/or hacking attack. Such firmware may be utilized, for example, for controlling the reading and writing of information to optional smart cards SC, the storing of voting record information in memory M, particularly, a specific memory device such as a memory chip card, an optical disk or tape, or other electronic, magnetic or optical media. Preferably, memory M of voting machine VM includes two independent non-volatile memory devices so that voting record information and a voting session identifier are stored on two separate, independent memory devices for redundancy and preservation of at least one copy of the accumulated voting records in the event one of the memory devices fails or otherwise becomes inoperative. Desirably, the two non-volatile memories are of different types, such as a semiconductor memory and a hard disk, or a memory card and an optical disk, or any other convenient combination.

Voter interface VI may be a standard or custom keyboard, as may facilitate write-in voting, or may be dedicated vote buttons or switches similar to conventional mechanical voting machines, for example, or may be a touch-screen interface associated with display unit DU, and is typically connected to processor P via cabling. Special keys can be provided for voting functions such as "Elect" or "Select" or "Vote," or for "Erase" or "Change," or for "Write-in." Alternative voter interfaces VI may include voice recognition apparatus, Braille keyboards or pen systems with writing recognition interfaces, each preferably with confirmation of the data entered displayed on display unit DU or even aurally via headphones.

Display unit DU may be of any suitable type, such as a conventional cathode ray tube or computer display, an LCD display, a touch-screen display or other suitable device, for displaying alphanumeric and/or graphical information, or a set of illuminated buttons, as desired, and is typically connected to processor P via cabling. Display unit DU may also include Braille devices, aural information via headphones, or other devices specially suited for people with handicaps.

Operatively associated with or coupled to processor P and memory M are a printer LP for providing a tangible record of the voting session, e.g., a printed paper receipt and an optional smart card reader/writer RW for writing and/or reading information from/to a smart card. Preferably, local printer LP and optional reader/writer RW are built into the physical container VMC of voting machine VM along with processor P, memory or memories M, display DU and voter interface VI, and that physical container VMC is rugged and scalable for security and to prevent unauthorized access to the components therein, thereby being resistant to tampering. Other components of a voting booth, such as a privacy curtain, an opening and closing mechanism therefor, and a floor stand, need not be part of voting machine container VMC, but may be permanently or demountably attached thereto as is convenient and desirable.

Optional smart card reader/writer RW is operatively associated with or coupled to processor P and memory M for writing information including at least a unique voting session identifier and a voting record into the memory of a smart card SC and optionally for reading information, such as voter registration and/or

identifying information, from a smart card. Each voting session identifier is a randomly-generated unique identifying or serial number or character sequence (e.g., a pseudo-random number) of at least eight characters or digits, and preferably of 12 or more characters or digits. Such voting session identifiers are generated for each voting session of each election, either centrally and then loaded into memories M of voting machines VM or by processor P as each voter participates in a voting session. It may be desirable for the voting session identifiers to include additional characters identifying voting district and /or the polling place and/or the voting machine VM on which the vote associated with the identifying number was cast, and/or the date and time of the voting session, but not the voter, so as to preserve voter anonymity while providing traceability of voting records. If any information particular to an individual voter is stored in the memory of smart card SC, as may be the case where information confirming voter registration or an identifying PIN number, security code or other personal data is utilized, such information is written over or erased or otherwise rendered permanently unrecoverable either before or at the time that voting record and voting session identifier information is stored in the memory of smart card SC by reader/writer RW of voting machine VM.

If reader/writer RW is a contact-type reader for use with contact-type smart cards, then the smart card SC is inserted into slot S thereof to be read and/or written to. If reader/writer RW is a wireless or contact-less -type reader for use with wireless or contact-less-type smart cards, then the smart card SC is placed proximate to antenna AN of reader/writer RW to be read from and/or written to. If reader/writer RW is of a type for use with both contact-type and wireless or contact-less -type smart cards, then the smart card SC is inserted into slot S if it is a contact-type smart card and is placed proximate to antenna AN if it is a wireless-type smart card, or is either inserted into slot S or is placed proximate antenna AN if it is a so-called "combi-card" that combines both external contacts and an internal antenna so that it can be read from or written to either via contacts or a wireless communication.

Further, while optional smart card encoder RW need only be able to write information to a smart card, it may also read information stored in a smart card SC and provide same to processor P. Reader/writer RW may also be a decoder to decode

information read from a smart card SC in encrypted or encoded form, and/or may also be a coder that encrypts or encodes information being written to the smart card SC. Such encryption and/or encoding may use public key encryption or any other suitable encryption and/or coding arrangement. Optionally, and preferably, reader/writer RW may include a "take-in" or capture mechanism that grabs smart card SC when it is inserted into slot S and, after the voting record and voting session identifier information is stored in the memory of smart card SC, deposits smart card SC into a secure collection box CB operatively associated with reader/writer RW and located in voting machine cabinet VMC. If this option is utilized, and it may be utilized with either contact-type or wireless smart cards SC, a separate collection box CB and action by each voter to deposit his or her smart card SC therein is not needed.

Local printer LP provides a tangible independent record of each individual voter's voting selections associated with the voter's unique identifying number. Printer LP is of a type that retains no record of the data printed (e.g., is not a daisy wheel or other printer employing a ribbon or other sheet-type ink source from which information printed may be extracted or reconstructed) such as a thermal printer, a dot matrix printer, an ink-jet printer, a bubble jet printer, a laser printer and the like, which are conventional. A specialty or security-type of paper, or other medium making authentication of a printed receipt easier and counterfeiting of altering of same more difficult, can be utilized, thereby reducing the likelihood of counterfeiting or fraud. Desirably, printer LP also prints information identifying the election district, the date and time of voting and similar information that may help to authenticate printed receipt PR. Exemplary voting receipts are illustrated in FIGURE 2A.

Preferably, voting machine VM displays on display DU the voting record of the voter and requires at least one confirmation, and preferably a second confirmation, of by the voter that the displayed voting record is indeed the vote(s) the voter intended to cast, in order to end a voting session. Information as to any offices or questions or referenda with respect to which a vote has not been cast can also be displayed and called to the voter's attention before the voting session is concluded. Upon the voter confirming the voting record, the electronic data thereof is provided to

the memory M of voting machine VM and to printer LP to be recorded on the voter's printed receipt with the voter's unique voting session identifier. Where optional smart card reader/writer RW is employed, the same data as is stored in memory M is encoded into the memory of smart card SC. Preferably, the same electronic data provided to display unit DU to be displayed to the voter is communicated to both printer LP and to optional reader/writer RW over a common path so there is certainty of consistency, although this is not necessary as it may be convenient for processor P to provide such electronic data in the particular forms required by a standard card reader/writer RW and a standard printer LP, rather than to provide a customized reader/writer RW and a customized printer LP each having a customized electronic data interface.

"Write-in" ballots can be accommodated by a special entry column that comes after the listing of all the named candidates. Any write-in voting can be done through the use of the keyboard or touch screen or other suitable means of data entry associated with voter interface VI and/or display DU. In this case, the "write-in" will typically include the last name along with first name of the person for whom a write-in vote is being cast, and, optionally, a middle name or initial, as is required by law and is common in conventional write in voting. The tabulation of write-in votes can be done manually or through processor P utilizing the same data base and polling software that records non-write-in votes, or by any other suitable methods and means.

The preferred VOTE-TRAKKER™ voting system and apparatus as illustrated by FIGURES 1B and 2 provides at least double redundancy for voting record and voting session identifier data in that each vote is recorded by at least two independent and verifiable means: to wit, by electronic recording in one or more electronic memories included in each voting machine, and by a confirmatory printed or other tangible record provided to each individual voter. Desirably, the preferred VOTE-TRAKKER™ voting system and apparatus as illustrated by FIGURES 1A and 2 provides triple redundancy for voting record and voting session identifier data in that each vote is recorded by at least one additional independent and verifiable means: to wit, by electronic recording in the memory of a smart card separate from the voting machine and the printed record. This apparatus, and the process and method it

performs, provide 100% transparency of each and every vote and maintains 100% privacy and confidentiality of each and every voter and vote.

FIGURE 3 is a schematic flow diagram illustrating the voting method 100 according to the invention. A voter registers to vote 110 and during the appointed times for voting, presents appropriate identification at the polling place so that his or her voter registration is verified 120 in accordance with the applicable law and procedure. Having properly done so, the voter is authorized to vote by the election officials and utilizes the voting machine provided for having a voting session 130 during which the voter makes his or her voting selections. As part of the voting session 130, a unique voting session identifier as described herein is provided for each voter and is associated with the voting record of that voting session which represents the voting selections made by the voter.

If an optional smart card or secured identity card is utilized, it is provided to each voter to serve as identification of the voter and proof of registration to vote. Each smart card is encoded with at least a specific assigned unique voter identifying number of at least eight digits, and preferably at least 12 digits, for tracking and future reference, and all smart cards for a particular election and polling place may also include the same particular security code or identifier that cannot be changed and that identifies the authorized polling location and election for which the smart card is valid. Each voter's smart card is utilized at the end of that voter's voting session 130 to record that specific voter's voting choices (voting record) and voting session identifier for subsequent use, if necessary, in recounting or verifying the votes cast, or for other challenges to the voting process. The voting record and/or voting session identifier is preferably written over any information such as a voter identification number that if not rendered unreadable would or could be utilized to ascertain from the smart card the identity of the particular voter who used it to vote. Optionally, an electronic marker, which may be the voting record or voting session identifier or any part thereof, is written into the memory of the smart card when it is utilized to cast a vote, to avoid its use for more than one voting session. Because the smart card includes a read/write memory, it may be erased and thus be recycled and reused for subsequent elections.

If utilized, a secured memory or processor chip card (or tag), i.e. a smart card, is issued 110 to each registered voter before the time for voting, i.e. prior to commencement of the period during which voters may cast their votes or at registration. A secured memory or smart card with an embedded electronic integrated circuit (IC) having substantial memory capacity, for example, over 1 kilobyte of memory, is preferred. For example, types SLE4442 or SLE4428 memory ICs available from Siemens, or other suitable equivalent, may be utilized. This memory bank IC is used for storing the voter's identifying number (ID) and the election/polling place security code before the card is used to vote, and after being used in a voting session stores the voter's voting selections, i.e. a voting record, and the voting session identifier, for subsequent recount, if necessary. The secured memory card should be issued anew with a new suitable and specific "Personal Security Code" or other unique identifying number for each election, for the purpose of providing a high level of security. Voting district or other political sub-divisional information, or other personal or social data, such as the voter's name, address, height and weight, eye and hair color, sex, birth date and age, a digitized photo, and the like, may also be stored in other portions of the smart card memory and may be utilized for providing a more secure election and election records as well as a improved identification of the voter, however, such information is preferably erased or otherwise rendered unreadable when the card is utilized in a voting session so as to preserve the voter's anonymity.

On election day, if the optional smart card is utilized, each registered voter presents 120 the pre-issued smart card with appropriate identification, if required, to the election officials at the polling place. A smart card reader may be utilized to verify the identity of the voter (i.e. of the person to whom the particular smart card was issued) and the validity of the smart card, as for confirming proof of identity. This optional verification and confirmation may be performed prior to the voter entering the voting booth or in the voting booth by the voting apparatus thereof, either by comparison to registration and/or personal information previously stored in the memory M of the voting machine VM or by communication link to a computer having a memory containing such information.

The voter now enters the voting booth or voting apparatus in order to vote 130. The voting session generally includes inserting the optional smart card, if utilized, into the voting apparatus, optionally verifying the voter's registration to vote, the voter making his or her voting selections, and the voter confirming the voting selections to end the voting session and establish the voting record of such selections. Specifically, the voter may enter an identifying number or may insert the smart card into the voting booth smart card reader to initiate a voting session 130. Based upon the information entered or read from the smart card, the voting apparatus through the voting system, may optionally make comparison of such information with official registration information. If the voter is correctly and properly registered to vote and if the information and/or smart card is proven valid, voting information will appear on a display screen of the voting apparatus for voter selection and voting. Voting information may appear all at one time for all offices, referenda, public questions and the like, or may be presented to the voter sequentially one office or question at a time. Once the voter makes a selection, the selection may continue to appear on a portion of display screen, e.g., with highlighting, while other selections are made or are made available one category at a time.

Once the voter has responded to all selections, all of the selections made will appear on the display screen for easy verification. If desiring to change any selection, either because a mistake has been made or he or she has changed his or her mind, the voter may select a "change button" to repeat a selection of a particular category or may select a "start-over button" to start the whole voting process again or may simply press the same button as previously pressed to make a selection to un-make that selection. The change and/or start-over buttons may be used at any time during the voting session, or at the end of making selections, and the button(s) may be physical buttons or touch zones on a touch screen display. If the voter confirms the selections by selecting a "confirmation" button or "confirmation" area on a touch-screen, the voting session is ended and the voting record and the voting session identifier generated by the voting machine are stored 170 in the non-volatile memory of the voting machine. If desired, a second confirmation could also be utilized. The same voting record and voting session identifier are also transferred 170 to a central

computer via a local area network within the voting facility or at a central voting facility, either as each voter completes a voting session or at the end of the voting period, as desired. Continuous connection to a location outside the voting facility should be avoided to prevent and/or reduce the likelihood of computer hacking or other outside attack on voting information.

Substantially contemporaneously with termination of the voting session, the same voting record and associated voting session identifier as are stored in the voting machine non-volatile memory are also written 140 to a tangible record, i.e. a printed copy for ease of voter verification of the vote as recorded. The voter may keep the printed record for his/her own reference. The voting records of all the voting sessions are tabulated or tallied 170 at the conclusion of the voting period for voting.

If the optional smart card is utilized, the same voting record and associated voting session identifier as are stored in the voting machine non-volatile memory are also written 150 to the memory of the smart card. After confirming his or her vote at the end of the voting session, if the voting apparatus does not automatically collect 150 the smart card, the voter is required to deposit 150 the smart card into a secure collection container before leaving the voting area. The smart cards containing the voting records of each specific voter are used for recounting 170 if the voting is challenged, and provide a separate and independent record of the voting records for such purpose. Once the election is over and the result officially certified, the information written to the smart card memory can be erased and, if desired, the smart card can be "recycled" for subsequent usage, e.g., in a later election.

Once the vote selections are confirmed, the voter is finished voting and the printed or other tangible record is made 140. If the law allows, however, the invention provides a safeguarded way for the voter to correct or change his or her vote, at least if the smart card, if utilized, has not yet been collected 150. A voter who realizes he or she has made a mistake or who has a change of heart regarding his or her vote may call upon an official in charge of the election for help to void or erase the previously cast voting record and to start his or her voting session all over. Preferably, the voting record of the second (correction) voting session is recorded along with the voided voting record from the first voting session and the respective

voting session identifiers for both the original voting session and the corrective voting session. The voided voting record from the first voting session is not actually erased, but is retained in the voting apparatus and is not counted in the vote tabulation, along with identifying information read from a smart identification or control card issued to the election official who authorizes the corrective voting session.

To enable the voting apparatus and system for such corrective voting session, the election official must insert his control card along with the voter's voted smart card, if utilized, to select and void the voting record already stored in the computer memory and remove it from the official voting records to be tallied and to allow the voter to repeat the process of voting. The changed voting record will be stored in a separate data base for use in constructing a history of the voting record, along with the voting session identifier and the identifying information from the election official's smart card.

In addition to the voting records of an election, the respective tabulations and tallies thereof may also include the voters' unique voting session identifiers for ease of inspection of voting records by the voter for confirming their accuracy. Such tabulated voting records serve as a public right-to-know record as well as maintaining the secrecy of voter's choice because only the voter knows his unique voting session identifier. If desired, demographic and other social data and the voter's corresponding choices may also be tallied as part of the voting record, if useful and allowed by the voting law and regulations, recognizing that such information is generally irrelevant under systems of law as in the United States and its maintenance derogates privacy.

A suitable relational data base, such as "Access" available from Microsoft Corporation or " Oracle" available from Oracle Corporation, may be utilized to record and tabulate voting records, depending on the size and complexity of the data being sought after. For most elections involving a population or political sub-division of less than about 10,000,000 people, a simple Microsoft Access data base may be adequate. Data base software and other computer programs may be provided as firmware so as to better secure the programming and to help to eliminate or reduce the possibility of tampering.

For absentee voting 160, voters may request a voting registration number or smart card in advance of the election similarly to the timing for conventional absentee ballots. Absentees may vote in any compatible specially designated voting booth that may be located in any convenient location so long as it is under the necessary control as required by the voting law, e.g., under personal control of a state election official. Because demographic information, such as the voter's home address and voting district, may be stored in the smart card along with other voting information, such designated smart card voting machine may be utilized by voters from different voting districts, different counties, or even different states, if desired. For example, a smart card voting machine could be located on a military base or in an embassy or consulate in a foreign country for use by all armed forces embassy and civilian personnel assigned to the base, embassy or consulate, as well as by their authorized dependents.

Alternatively, absentee voters may use the traditional mail-in paper ballot in the conventional manner, with or without an officially-issued smart card for processing the absentee ballot. One or more election officials having one or more "official's cards" will insert such official's smart cards into the voting machine and cast a vote as prescribed by the paper absentee ballot for such person following exactly the same voting process as described above. The voting record and voting session number for each such absentee voting session, which include information from the official cards identifying the official entering the absentee voter's vote, are stored in a separate data base and are tabulated with the voting records from the standard voting 120-150. As a result, any subsequent challenge or recount can be easily monitored with detailed voting records of absentee votes and regular votes.

FIGURE 4 is a schematic flow diagram illustrating the voting method 100 according to the invention in greater detail. Although FIGURE 4 illustrates the utilization of an optional smart card, it is understood that the method of FIGURE 4 may be practiced with or without a smart card. Initially 102 , the voter presents proof of citizenship and residence as is necessary for registration to vote, and alternatively, satisfies any other requirements for registration for voting and issuing 110 of a voter registration. If smart cards are utilized, the voter could be issued a smart card at this time or prior to the election, as is desired. Such registration may include, for

example, connection and providing of information through a local area network with the computer that will ultimately be tabulating the voting along with the voters' unique identifying (serial) number, i.e. registration number, so that eventually, all voter registrations are recorded on the central computer for the verification 114 of voter registration and/or ultimately, during and/or after an election, the storing/recording 138 of voting results. The stored voting results include but not limited to each voter's voting record and voting session identifier, i.e. unique identifying serial/identifying numbers, which may be published 180 or/and posted in public location and/or posted 180 on a special election web site for examination by the voters and other members of the public.

Election officials may issue a unique voter-identifying serial number or registration number or voter number for the registered voter, or a voter card or "voting ticket" with the voter's personal data thereon for verification 114 of voter identity. An election official may type in the serial or other number of the registered voter to verify 114 registration before allowing the voter to vote. This verification module may be linked to a registration data base that is separate from the voting machine, such as in a central election computer. The election official then issues 112 to the voter an authorization to vote. If smart cards are utilized, such authorization may include a chip card or smart card with the same unique identifying serial number and personal identification data (e.g., similar data to that of driver license for ease of verification by the voting attendant or election official). Alternatively, any other suitable verification criteria, including signature comparison, driver's license identification or the like, may be utilized to authenticate 114 the voter's registration, in accordance with the applicable election law and voting procedure, and to issue 112 a voting authorization and/or smart card to the voter.

If utilized and alternatively,, a chip card (i.e. smart card) is issued 112 to the voter with a unique identifying serial or registration number and, optionally, personal identification data (e.g., similar data to that of driver license) for ease of verification by the voting attendant or election official. The voter takes the smart card to the polling place, verifies registration 114 and then inserts the chip card into the smart card reader/writer of the voting machine to activate 132 the voting machine to initiate

and engage in a voting session. Alternatively, the voter may insert the chip card into the smart card reader/writer of the voting machine to verify 114 registration to vote and activate 132 the voting machine to initiate a voting session

It is noted that while the chip card is preferably used as a repository of a separate voting record electronic file, its use is optional depending on the level of voting record redundancy required and/or desired.

The next step is for the voter to vote 130. The voter initiates 132 a voting session, such as by pressing a button, by moving a lever or handle or switch, or by entering an identifying number, personal security code (PSC), personal identifying number (PIN) or the like. If a smart card is utilized, inserting the chip card can activate the voting machine to begin/initiate a voting session 134. The voter votes 134 by making selections for election of the candidates for different posts or offices, and/or for public questions, constitutional amendments and the like. Alternatively, the voter can elect to make a write-in entry for a candidate not listed on the predetermined ballot. Suitable means of voting data entry include but are not limited to a touch-screen, a "point-of-sale"-type special keypad, a standard keyboard, voice-recognition, a specialty keyboard for handicapped persons (e.g., a Braille keyboard for the blind).

Before a voting session is completed, the voter confirms 136 the voting selections he has made. If the voter does not confirm 136 his selections (path "N"), the voting machine allows him to change his selections and/or make additional selections. If the voter confirms 136 his selections (path "Y"), the voting session is complete and the voting record along with a unique voting session identifier generated by the voting machine are stored 138 in the memory devices of the voting machine and are also provided to produce 150, 140 at least one separate tangible record of the voting session. A printer is utilized to provide 140 a tangible printed receipt including at least the voting record and voting session identifier, and may also include election and voting information such as date, time and polling place location. Where smart cards are employed, at least the voting record along with the unique voting session identifier is also provided 152 the smart card reader/writing device to be stored in the smart card which is collected 154. All "raw" voting records are

preferably stored 138 within the voting machine by suitable means of electronic data storage that are redundant so as to provide a stored voting record and voting session identifier that are separate from and will be available as a back-up to the computer storage thereof. The stored 138 voting record data is available anytime later, should it be needed, as for a recount or challenge.

The tangible receipt device provides 140 a tangible receipt such as a printed receipt. The smart card reader/writer erases personal data, if any, stored on the voter's smart card and encodes 152 the voters selections 134 and voting session identifier on the card memory for future use, such as for electronic recounts. The smart card is collected 154 , either automatically by the card reader/writer or by the voter depositing the smart card into a secure collection box. The voting machine memory as well as both the printed receipt and the encoded information stored in the smart card include the same voting session identifier which is a serial number as issued by the voting machine or a randomly generated unique identifying serial number generated from a defined set that is associated with the particular voting record if absolute privacy is preferred. The voting session identifier or serial number may include identification of state, county, precinct, or other appropriate political sub-division, along with the random portion of serial number assigned to assure privacy, such as is illustrated in FIGURE 2A. The time and/or date of voting may also be optionally recorded on the printed receipt and in the voting record stored in the voting machine, the smart card, or both, for future inspection and/or verification.

If the period for voting has not ended, the poll open test 139 is affirmative (path "Y") and the voting machine is available to the next voter. If not, the voting machine accepts no further voters (path "N") and the vote is tabulated 170. The determination of poll open or not may be by local timer, voting official deactivation of the voting machine or signaling from a central election location and/or computer.

The confirmed 136 voter selections are tabulated 170, for example, via a local area network connection to a computer for tabulating the voting along with the voters' identifying serial numbers. Eventually all voting records are tallied 170 along with the voters' voting session identifiers or serial numbers, and can be published 180 for examination by the voters or other members of the public. Such publication 180 may

include distribution of printed copies and/or posting copies in a public location or on a special election web site on the Internet. The voting process ends 190 when all of the voting records are tabulated and the election results are certified or otherwise made official and final in accordance with the election law.

Absentee voting is provided 160 by conventional paper ballot 166 or by smart card issuance 168, as is desired. An absentee ballot is requested 162 and election officials determine 164 (or have predetermined) whether a conventional paper ballot or an optional smart card should be issued. If a paper absentee ballot is not to be utilized (path "N"), a smart card is issued 112 and the voter utilizes the smart cord to vote 130 as described above, for example, although the authorized voting machine may be in the voting district or remote from the voting district, as described above, or the voting 130 may be performed in advance of or at a different time from the normal election day voting period.

FIGURES 4A-4D are schematic flow diagrams illustrating further details and alternatives for the voting method 100 of FIGURES 3 and 4. FIGURE 4A illustrates an alternative to on-site verification 114 of voter registration by the election officials presiding at that place. The officials or a data entry device at the polling place receives 114A verifying data from the voter and that data is transmitted 114B to a central computer in which resides files identifying properly registered voters. The central computer checks the voter's data to verify registration to vote and provides 114C verification of registration to the polling place. If smart cards are utilized, verification 114 may be before or after issuance 112 of a smart card to the voter.

FIGURE 4B illustrates alternative steps for issuing 112 an optional smart card in which a unique voter identification number is issued 112A and then voter data is entered 112B into the voting system. The data entered is stored 112C in the memory of the smart card and the smart card containing such data is then provided 112D to the voter, who may thereafter utilize it for verifying registration and/or in voting.

FIGURE 4C illustrates alternative steps for storing 138 voting record and voting session identifier information at the conclusion of a voting session. When the voter has confirmed 136 his voting selections, the voting record thereof and the voter's voting session identifier are stored 138A in the memory device or devices of

the voting machine, i.e. locally, and are also transmitted 138B to a central election computer. The central computer stores 138C the voting record and voting session identifier and also "flags" or marks 138D the registration record of that voter to indicate that the voter has voted in the election. Optionally, the central computer may confirm 138E to the voting machine computer that the voting record has been centrally stored and/or confirm 138E that the polls are still open to enable voting by additional voters. One advantage of this arrangement is that by marking the voter's registration to indicate that the voter has voted, further attempts by the voter to vote will be rejected, thereby eliminating any voter voting more than once. Thus the old cynical saw, "Vote early, vote often," can no longer be applicable.

FIGURE 4D illustrates alternative steps for verifying voter registration as part of each voter's voting session. In voting 130, the voter enters 132 his voter identification information or inserts 132 his smart card into the voting machine to open it for voting. Before the voting machine opens for voting 134, the voter's registration is verified 114, either by reference to registration data stored in the voting machine or via central verification 114 of the sort described in relation to FIGURE 4A. A voting session is initiated only if and when the registration is verified 114.

The present invention can be embodied as a computer implemented process or processes and/or apparatus for performing such computer-implemented process or processes, and can also be embodied in the form of a tangible storage medium containing a computer program or other machine-readable instructions (herein "computer program"), wherein when the computer program is loaded into a computer or other processor (herein "computer") and/or is executed by the computer, the computer becomes an apparatus for practicing the invention. Storage media for containing such computer program include, for example, floppy disks and diskettes, compact disks (CD)-ROMs (whether or not writeable), DVD digital disks, RAM and ROM memories, computer hard drives and back-up drives, and any other storage medium readable by a computer. The invention can also be embodied in the form of a computer program, for example, whether stored in a storage medium or transmitted over a transmission medium such as electrical conductors, fiber optics or other light conductors, or by electromagnetic radiation, wherein when the computer program is

loaded into a computer and/or is executed by the computer, the computer becomes an apparatus for practicing the invention. The invention may be implemented on a general purpose microprocessor or on a digital processor specifically configured to practice the invention. When a general-purpose microprocessor is employed, the computer program code configures the circuitry of the microprocessor to create specific logic circuit arrangements.

Accordingly, the voting system and method of the invention may be provided on such computer storage media for causing voting apparatus to operate responsive thereto in performing the invention. While the voting device utilized by the voter is referred to herein as a "voting machine," the voting machine is not wholly mechanical but is partially or wholly controlled and operated by a computer or processor. Thus, the invention may be implemented by providing an appropriate computer program to an existing voting machine or apparatus, such as in the form of a read-only memory device or module or other firmware, a floppy disk or other magnetic media, and CD-ROM or other optical media and the like, or by a communication utilizing an electronic and/or optical communication path.

Voter Registration and Smart Card Issuing: Similarly to the current voter registration process, each individual voter is mailed a voting ballot sample that reflects the actual voting ballot to be utilized in the official election. A smart card is encoded with a unique serial number, such as a voter identifying number, and is issued for each individual voter. This serial number has at least enough digits for representing the voting population, e.g., at least 8 digits, and preferably 9 or more digits, e.g., for anonymity. If the set of unique serial numbers may be utilized as voting session numbers, which is not preferred, the numbers should be independently generated anew for each election, and should not be related to the voter's traceable numbers, such as social security number, telephone number, address and the like. It should be used by and only be traceable, if at all, at the voter registration office, i.e. by election officials, and should be strictly controlled for security and protection of voter privacy.

Optionally, information regarding each voting district can be encoded into the smart card with another set of numbers that represent such district and its political

sub-division, such as voting precinct or other specific voting related information. The serial numbers may be optionally published, for example, with the vote tallies and records of each individual voter's choice associated only with the anonymous voter's serial number (voting session identifier) may be posted in the Internet for absolute transparency of voting records and yet maintain the privacy and confidentiality of each voter's choices. Any dispute or challenge to any particular voting record, if permitted, must be made with the printed receipt that the voter was issued at completion of the voting session and is retained for verification, because the voter's printed receipt contains the same voting record and unique identifying number (voting session identifier) with which the voter's smart card was been encoded. The voting record stored in the smart card and printed on the voter's receipt may also include the date and time of voting and/or the identity of the polling place, voting district and voting machine, as desired. The medium on which the printed receipt is printed may have security indicia or other authentication or security features, if desired.

After the voting result has been certified and the time for challenge of the correctness of the election has passed, the information stored in the smart cards may be erased and the smart cards recycled for the next election. Each election should use a different identifying number or special personal security code (PSC) for each voter that cannot be modified easily without knowing the original code, which is known only to the election officials, and thus no confusion will ever occur, e.g., between voters in any one election or between voters in different elections.

The unique serial number assignment for each voter and the electronic record of the voting which includes the fact that particular serial numbers have been used to vote can, e.g., if utilized to verify eligibility to vote at the beginning of each voting session, eliminate any possible double voting or unauthorized voting.

If the smart card is mailed to the voter and is claimed to be lost, a separate replacement smart card may be issued to the voter at the election site, similar to the so-called "provisional" ballot utilized in some voting districts. The lost smart card serial number will be noted, and, optionally and preferably, may also be voided for the purpose of the present election. More security and control may be exercised where the issuing of replacement smart cards is made only with two election officials

inserting their special election officer smart cards to enable the issuance of the voter's replacement smart card. The record of issuance of a replacement smart card will be listed as a separate record in the voting records stored in the voting machine and/or the central voting computer for ease of inspection and verification.

Specialty voters such as the "domestic absentee" and "overseas absentee" are issued specially serialized paper ballots and optionally, corresponding smart cards. Their votes will be made on the paper ballot and mailed back to the respective voting district or other proper election authority. Alternatively, the same smart card electronic voting facilities as are utilized in the home election districts may be made available at dedicated places outside such districts. For example, special voting locations can be made available such as at a local consulate or embassy of the country, and citizens in that place during the time for voting may vote there utilizing the absentee smart card received by mail.

If serialized paper ballots are used along with the serialized smart cards, the actual voting tally may be made with appropriately secured and supervised official tabulation at the voting district. The same voting and tabulation process as described above may be utilized, and the same transparent voting records are also available for the voter's inspection, e.g., via the Internet. All ballots voided for whatever reason may also be likewise posted for the same transparency.

Off-site and/or off-day voting may also be permitted. If the local or national laws allow, voting machines may be placed at locations other then the conventional polling centers. These sites may include police stations, post offices, schools, banks, and other suitable public locations with reasonable supervision and assistance to the voters. The voting can be done anytime, including days other than the general voting date, and could be for an extended period, e.g., for one or two weeks. The votes so cast will be verified and approved if the voter's smart card (chip-card) has been returned (collected) and the voting record stored therein matches when compared with the voting record stored in the voting equipment and/or the optional central computer.

Electronic Re-Counting: If the electronic tallies of voters' choices as produced from the voting records stored in the voting machines is ever challenged, the optional collected smart cards may be read and easily tallied again for

comparison, either as to accumulated voting results or on a vote-by-vote basis using the unique identifying number (voting session identifier). In fact, if desired, all the collected smart cards may be read and counted after the electronic tallying to verify the accuracy of the voting machine results. If any smart cards are missing (e.g., not collected or lost), they can either be readily verified for the record from the voting records stored in the voting machine or the vote can be disqualified.

If there is any challenge or discrepancy claimed by any voter, the challenged vote can be compared with the printed receipt that must be presented by the voter for making such claim which includes the specific serial number (voting session identifier) and the voter's choices corresponding to those stored in the respective memories of the optional smart card and/or the voting machine. The electronic voting records can be easily tallied and listed, and corrected, if appropriate, and may be published and or posted via the Internet to ensure the absolute transparency of the voting.

It is noted that the smart card can be read accurately almost 100% of the time and can be essentially absolutely error free. Conventional error reduction techniques such as comparison of multiple readings and error checking codes, or both, may be employed as is convenient and desirable.

It is preferable that the voting machine be able to automatically take-in the smart card (chip card) once the voter is finished voting. In the case where a semi-manual voting machine is used, e.g., where the voter is required to deposit his smart card in a locked collection box after voting, it may be required that if the smart card is not returned, the validity of the vote is lost, i.e. the vote may or may not count, depending on the law. Alternatively, the voting machine can be programmed so that the return of the voter's smart card must be made before the next voter can use the voting machine, e.g. as part of a double checking process for collecting smart cards. Once the voting time is over, the electronic tally of all voting is immediately available for each district from the voting machine(s) thereof and may be transmitted electronically to an election headquarters or other facility for making a total tally of the voting. All voting tallies may include the serial number (voting session identifier) of each voter for absolute transparency.

All smart cards utilized in voting are to be locked up and kept under security similar to that utilized for conventional paper ballots today. They can be automatically read and counted or recounted using an automatic smart card encoder unit or a smart card printer-encoder or reader such as those available from Fargo Electronics, Inc. located in Eden Prairie, Minnesota, or from Atlantek, Inc. located in Wakefield, Rhode Island, or from Avante International Technology located in Princeton, New Jersey.

Alternative Media for Paper Ballot Replacement: The use of smart cards as part of the voting process can dramatically help to eliminate any doubt about the validity of the vote and the voting result, and is a great improvement over current election processes, especially those relying on paper ballots and punch card ballots. Instead of recording the voting record on an individual smart card that is mailed to the voter, the smart card may be utilized at the voting sites only. In that case, the unique serial number (voting session identifier) for each voter is generated and/or assigned during the voting process, e.g., by the voting machine during a voting session, with the voting record printed receipt having the same identifier for absolute transparency.

Alternatively, the individual voting record may be stored in the non-volatile memory built-in within the smart card (chip card) reader/writer, or alternatively, in the hard disk of the computer within the voting machine, preferably with built-in redundancy such as a parallel processor and/or non-volatile memory, or a combination of the above. In any case, the voting data should be stored as individual voter records associated with the voter's unique identifying serial number (voting session identifier) rather than as total or tally only. Also alternatively, the individual voting records may be stored in any other suitable electronic media, optical media, or even electronically or optically readable media printed on paper, as may be convenient, both within the voting machine or in the smart card.

FIGURE 5 is a schematic diagram illustrating a redundancy feature of the invention which includes triple voting record storage to ensure redundancy and security. Each voting record VR is produced by a voter making voting selections during a voting session and includes those selections as well as the unique identifying number (voting session identifier) issued to that voter. Voting record VR and the

voting session identifier associated therewith are stored in three independent and separate memories: at least one (and preferably more than one) in central computer 12, at least one (and preferably more than one) in voting machine VM and one in optional smart card SC. Optionally, information relating to the voting session, such as the date and time of voting, the voting district and polling place, and the like may be associated with each voting record in any one or more of the separate memories and on the tangible receipt, as may be desired.

Computer 12 is typically linked to plural or multiple voting machines VM. Each of the voting records VR and voting session identifiers from each of the voting machines VM is down-loaded to computer 12 either immediately after each voting session or at the close of the voting period, such as via a conventional RS485 or RS232 electronic interface. All of the voting records VR and voting session identifiers are stored and tabulated by computer 12, such as by a relational data base such as "Access" or "Oracle". All of the tallies are eventually combined at the election headquarters or other official election site, i.e. usually where computer 12 is located. All voting records, voting session identifiers, and tallies thereof are made public with reference to each voter's randomly generated serial number (voting session identifier) for 100% transparency of the voting.

Voting machine VM includes an independent memory storage device for storing for the raw voting data and the respective voter's serial number (voting session identifier) associated therewith. Preferably, voting machine VM includes at least two separate non-volatile memory devices so that the integrity of the stored voting records is maintained even if one of the memory devices should malfunction, fail, or be tampered with. Each of the voting records VR is also transmitted to the computer 12.

A printer or other device outputs a tangible record PR of the voting record VR that includes all the information that is stored in and resides in the voting machine and in optional chip card SC. The printed-out receipt PR is retained by the voter for reference and for checking his or her vote against the final posted voting tallies which include the voters' identifying numbers (voting session identifier). The printed-out receipt PR typically includes, for example, the voter's unique randomly generated

serial number (voting session identifier), all of the voter's voting choices (voting record), the time of voting, and other relevant data.

In addition, the same voting record VR and voter identifying number (voting session identifier) is optionally also recorded in the memory of smart card SC, i.e. using the chip card SC as a third separate and independent medium of storage. Each smart card SC represents one voting record VR and voting session identifier stored therein that can be electronically read even if the voting records stored in both computer 12 and voting machine VM are lost or corrupted for whatever reason, or if the election results need to be recounted or are challenged. Note that chip card SC stores an individual voting record VR including, for example, the voter's unique randomly generated serial number (voting session identifier), all of the voter's voting choices, the time of voting, and other relevant data.

While the present invention has been described in terms of the foregoing exemplary embodiments, variations within the scope and spirit of the present invention as defined by the claims following will be apparent to those skilled in the art. For example, the articles issued to individual voter's are referred to as cards, but need not be a card per se, but may be tags, sheets or articles of other suitable form providing a suitable voting record storage memory. Further, while the voting record is said to include the voter's identifying number and the voter's voting selections, the voting record may be related entries of the identifying number (voting session identifier) and the voting selections in a memory, such as in a computer relational data base.

It is noted that while the specific number, i.e. voting session identifier, associated with each particular voting record may sometimes be referred to as a "serial number," it is preferred that such numbers not be sequential or in any order that would allow relation of the voting record to a particular individual voter. Thus, a set of randomly-generated unique numbers or pseudo-randomly-generated unique numbers may be utilized and is preferred. A series or sequence of unique numbers (i.e. true serial numbers) could be utilized if the resulting loss of protection of voter privacy is acceptable, or if privacy is sufficiently provided for by security/secrecy of the numbers assigned. In addition, while "numbers" are referred to, such numbers

need not be numerical, but may be any combination of alphanumeric or other characters or symbols. Similarly, voter identifying numbers, security codes and the like may also be numeric, alphanumeric or symbolic, as is desired.

The apparatus, system and method of the invention provides a degree of security, privacy and transparency that is at least desirable, if not preferable or necessary for official governmental elections, the invention may be utilized for private voting, labor representation and union elections and any other polling even though such unofficial or non-governmental polling does not require such security, privacy and/or transparency.